SAND99-2085

Sandia National Laboratories

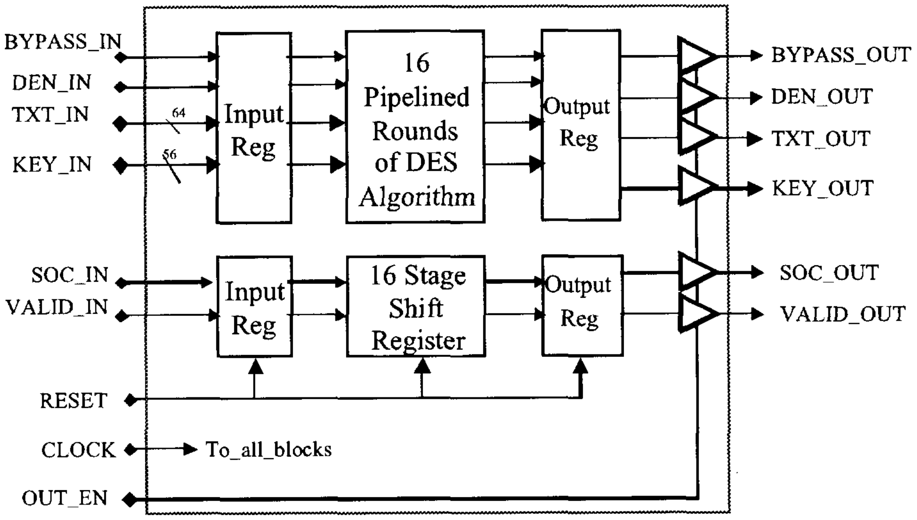
DES ASIC DATA SHEET

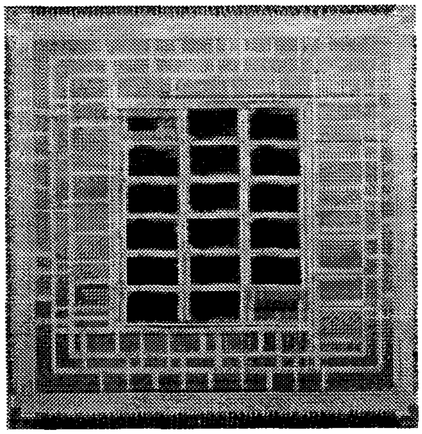
SEPT. 4, 1998

OVERVIEW:

The Data Encryption Standard (DES) as defined in the Federal Information Processing Standards (FIPS) Publication 46-1 is used for protecting data by cryptographic means. Sandia National Labs has implemented the DES algorithm in an Application Specific Integrated Circuit (ASIC). The design allows encryption, decryption, unique key input, or algorithm bypassing on each clock cycle. This is a 60K gate pipe-lined implementation having 251 IO signals and 68 power and ground pins. The chip has been fabricated in a 0.6 um CMOS process using a fully static design. This chip has been shown to operate as high as 105 MHz, yielding a single device throughput of 6.7 Gb/s. Six devices operating on an entire ATM Cell (384 payload bits in parallel) will yield OC-768c throughput of 40 Gb/s. While power dissipation at high throughputs is a challenge, the same device clocked at low speed can achieve encryption of multiple voice channels while consuming less than half a milliwatt of power.

FUNCTIONAL BLOCK DIAGRAM:





- Fully pipelined DES
- Triple-DES by cascading 3 devices
- 0.6 micron CMOS
- Die size: 11.1 mm square
- 319 total pins, 251 I/O
- 6.5 Watts @ 105 Mhz (6.7 Gb/s)
- Each clock cycle can:
    - Bypass
    - Encrypt/Decrypt
    - Establish new key
    - Flag Start of Cell (SOC)